BlueBorne vulnerabilities

BlueBorne is a set of vulnerabilities found in various OS implementations of Bluetooth stacks.

Info taken from *BlueBorne Technical Whitepaper*

Linux Kernel RCE

CVE-2017-1000251

Vulnerability in `BlueZ`, Linux bluetooth stack implementation. Buffer Overflow vulnerability in `l2cap_parse_conf_rsp` function. To trigger the vulnerable code path, attacker needs to set victim device into `Pending` state of EFS configuration process. However, this can be easily accomplished by sending a crafted configuration request.

According to `NIST` NVD, the last vulnerable version is `4.13.1`.

Armis Labs, the lab that discovered BlueBorne, states that the vulnerable feature was added in version `3.3`, however, `NIST` claims kernels from `v2.6.32` are vulnerable.

---

vulnerable from: `2.6.32`

vulnerable to: `4.13.1`

Linux Info Leak

CVE-2017-1000250

Another vulnerability in `BlueZ`. The vulnerability lies in `SDP` server implementation.

`SDP` - Service discovery protocol defines communication between client, who is sending `SDP` requests to server, who replies with services it supporst in `SDP` responses. In case the SDP response is longer than current negotiated `MTU`, mechanism called SDP continuation is used to transmit it. In SDP continuation, Server appends response with continuation structure and clients sends back the original request with the continuation structure it received. Thus, the server relies on client to send back the same structure.

The vulnerability lies in insufficient checks of this continuation structure received back from client.

To exploit this vulnerability, client sends malformed continuation structure back to server with e.g. wrong offset to leak memory from server's heap.

---

vulnerable to: `BlueZ` v5.46 released on 14/09/2017

Android Info Leak

CVE-2017-0785

This vulnerability relates to the same process as previous one, the `SDP` continuation. Despite validation of the offset value into the heap buffer, researchers were able to find and underflow vulnerability leading to information leakage.

According to `NIST` `NVD`

vulnerable from: `4.4.4`

vulnerable to: `8.0` incl.

Android RCE #1

CVE-2017-0781

`BNEP` (Bluetooth network encapsulationb protocol) finds most of its use-cases in internet tethering over bluetooth.

Vulnerability was found in handling of `BNEP` control messages. Researchers found particular piece of code that corrupts heap everytime it is run. However, this code has very likely never been run during testing. The code handles very special situation: when two `BNEP` control messages are received within one `L2CAP` packet. And at the same time, the connection state has changed after the first control message was handled but before the second is being handled. Very unlikely to happen in practice, unless deliberately. Thus, the attacker is very well able to reach the vulnerable code.

According to `NIST` `NVD`

vulnerable from: `4.4.4`

vulnerable to: `8.0` incl.

Android RCE #2

CVE-2017-0782

Second android RCE vulnerability also lies in `BNEP` implementation, this time it is an integer underflow of variable that holds remaining length of unprocessed packet when processing `BNEP` control messages. This underflow also leads to remote code execution, however, the exploitation is not trivial. Another fact that makes life easy for attacker is that the vulnerable code runs as 32-bit process, which makes `ASLR` bypass easier.

According to `NIST` `NVD`

vulnerable from: `4.4.4`

vulnerable to: `8.0` incl.

According to `NIST` `NVD`

Bluetooth Pineapple

CVE-2017-0783 & CVE-2017-8623

One of the bluetooth services, as mentioned earlier is internet tethering. The following vulnerability lies in insufficient security enforced on the tethering device. Based on service severity, it can define the minimal level of security that needs to be enforced on the lower layer to allow the service. For example, the service may be refused if sufficient authentication method was not used during the pairing.

However, this was not done in Android and Windows implementations of internet tethering enabling service. The researchers were able to connect to the victim device without victim noticing and function as man in the middle for the victim's device connections. The services' required security level was low enough to work with device paired via Just Works method which is easily done without victim noticing.

Android CVE-2017-0783

vulnerable: `4.4.4` to `8.0`

Microsoft CVE-2017-8623

vulnerable: Microsoft Bluetooth Driver in `Windows Server 2008 SP2`, `Windows 7 SP1`, `Windows 8.1`, `Windows RT 8.1`, `Windows 10 Gold, 1511, 1607, 1703`

Apple RCE

CVE-2017-14315

`LEAP` is Apple's low energy audio protocol, used to stream audio to low energy peripherals.

In received audio data handling. assumption on audio chunk length made by the implementers leads to Heap Overflow vulnerability. The assumption is correct, if the connected device is connected via `BLE`, however, for a `BR/EDR` connection, the limitations are not as low. Researchers state that most of the code validates the origin (`BLE` vs `BR/EDR`) of the incoming packets, however, this is not done consistently.

In the white paper, they state this was not exploited during the research.

---According to `NIST` `NVD`

According to `NIST` `NVD`

vulnerable from: iOS `7.0`

vulnerable to: `9.3.5` incl.

---

next: blueborne year later - multiple new vulnerabilities found after blueborne

https://armis.com/blueborne-one-year-later/